POLICY TITLE: Privacy and Confidentiality

PURPOSE:

The West Durham Family Health Team (WDFHT) and The West Durham Family Health Organization (WDFHO) are dedicated to quality patient care and improving the health status of our communities. A patient's right to privacy is balanced with the West Durham Family Health Team's and West Durham Family Health Organization's obligation to provide effective health care treatment.

POLICY:

The WDFHT and WDFHO abides by the *Health Information Protection Act* (November 2004), comprised of both the *Personal Health Information Protection Act* (2004) and the *Quality of Care Information Protection Act* (2004).

The WDFHT and WDFHO are responsible for the personal information and personal health information under its control and will in good faith endeavour to ensure that all personal information will be kept private, confidential and secure.

The WDFHT and WDFHO employees are accountable for maintaining confidentiality and privacy of all information collected, accessed or disclosed during and after their employment or professional contact.

All information collected, used, accessed or disclosed is protected as referred to in the following interrelated principles.

Principle 1 – Accountability for Personal Information
The WDFHT and WDFHO are responsible for any personal information in its possession including information that has been transferred to a third-party for processing.

The Executive Director will oversee the compliance to the policy, related procedures and legislation. The identity and contact information of this person will be made known to the public.

Principle 2 – Identifying Purposes for Collecting Personal Information
Personal information related to patients is collected, used, disclosed and retained for:

- Direct patient care,
- Administration of the health care system,
- Conducting risk management and quality improvement activities

- Research, teaching, statistics,
- To meet legal and regulatory requirements, and
- Fulfilling other purposes permitted or required by law.

Patients imply consent when they present for treatment and receive an explanation for the health services to be provided. Unless a new purpose is legally required, consent must be obtained before the information can be used.

Principle 3 – Consent for Collection, Use and Disclosure of Personal Information
The knowledge and consent of the individual is required for the collection, use or disclosure of personal information, except where inappropriate.

The WDFHT and WDFHO will inform its patients and clients and make reasonable effort, through reasonable means (i.e. signage, information brochures, WDFHT website etc.), the purposes for which the WDFHT and the WDFHO will use their personal information.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is collected for detection and prevention of fraud or for law enforcement, obtaining consent may defeat the purpose of collecting the information. Obtaining consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.

Personal information that has been collected for a purpose not previously identified will be made known prior to its use. Unless the new purpose is required by law, consent will be obtained prior to the use of the information.

Principle 4 – Limiting Collection of Personal Information
The WDFHT and WDFHO will limit the amount and the type of information collected to that which is necessary to fulfill the purposes identified. All information will be collected by fair, lawful and indiscriminate means.

Principle 5 – Limiting Use, Disclosure, and Retention of Personal Information
Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent from the individual or as required by law.

Personal information will be retained only for as long as is necessary for the fulfillment of those purposes or as required by law (i.e. legislative requirements with respect to retention periods of personal health records).

Principle 6 – Accuracy of Personal Information
Personal information will be as accurate, complete and up-to-date as possible and as is necessary for the purposes for which it is intended. Patients (or their substitute decision-maker) may request a correction to their PHI orally or in writing. This correction will be made only when the patient (or their substitute decision-maker) can demonstrate to our satisfaction that the record is not accurate or complete for our purposes and also gives the

information needed to make the correction. Any correction to PHI will be made by crossing out the incorrect information or labelling it as incorrect in the chart. Corrections will be dated when made.

Significant exceptions apply where WDFHT/WDFHO do not have to correct a record:

- If the record was not created by WDFHT/WDFHO staff
- Where WDFHT/WDFHO staff do not have significant knowledge, expertise and authority to correct the record (this would include when WDFHT/WDFHO cannot validate the new information provided)
- If a WDFHT/WDFHO staff reasonably believes that the request for correction is frivolous, vexatious or made in bad faith (requests should only be refused for these reasons in rare cases)
- If the patient has failed to demonstrate that the record is not correct or complete, or
- If the patient has not given WDFHT/WDFHO the information needed to make the correction.

Note: WDFHT/WDFHO do not have to correct a professional opinion or observation made in good faith about a patient. The WDFHT/WDFHO's Statement of Information Practices will inform patients/substitute decision-makers whom they can contact if they want to correct their PHI. All staff and health care professionals will be trained on how to ensure accuracy of PHI.

Principle 7 – Safeguards for Personal Information

The FHT has security safeguards in place to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification regardless of the format in which it is held. Care will be used in the disposal or destruction of personal information to prevent unauthorized persons gaining access to the information.

If a patient's PHI is stolen, lost or accessed by unauthorized persons, we will notify patients.

Reasonable steps that will be taken to ensure physical security. The following is a list of some of the steps we take:

1) Physical files containing PHI will be locked/and or /supervised.
2) Printer/fax machines will be monitored and placed in secure areas
3) Access to offices are restricted
4) All contractors and third parties who have access to the site for approved work sign a Confidentiality Agreement which includes compliance requirements for PHIPA
5) Shredding machines and off-site shredding disposal are used for disposing of any PHI
6) All computer hardware that is no longer in use will be destroyed according to PHIPA standards.

Reasonable steps will be taken to ensure technological security of PHI. The following is a list of some of the steps we take:

1) Each staff member will have their own User ID/Passwords to access PHI and be instructed never to share their Password.
2) Staff will be instructed how to create acceptable Passwords and how to change them periodically
3) We will utilize up-to-date anti-virus firewall and spyware software on computers.
4) Staff will not install any unauthorized software or connect any unauthorized devices to their computer or use their computer for unauthorized purposes.
5) All staff upon hiring, sign the Acceptable Use Policy for Computers and Internet in Medical Practices.
6) Staff cannot copy or transmit externally any PHI from their computers unless authorized (including e-mail and instant messaging) and if authorized (eg. Transmitting OHIP billing), will use encryption and/secure site (eg. VPN)
7) Staff will be advised to be aware of the "reader over the shoulder" and neighbours overhearing loud conversations.

Steps will be taken for administrative controls. The following lists some steps we will take:

1) Criminal Checks will be conducted for all WDFHT staff. Reference checking will be completed for all new employees.
2) Employees will have a Confidentiality/Privacy protection clause included in their Employment Contracts.
3) Upon hire, staff will sign a Confidentiality Agreement acknowledging their understanding of the WDFHT/WDFHO Privacy/Confidentiality /Security policies and procedures.
4) Employee access to PHI will be restricted based on the scope of practice and job responsibility.
5) Employees will receive privacy/confidentiality/security training.
6) Employees will receive a unique building security alarm access entry card and code. Employees are instructed to keep the Alarm Security code separate from the actual Security Card.
7) Employees are instructed to immediately notify management if the Security Card is lost or stolen. All misplaced Security Cards are immediately deactivated.
8) Access to the clinic will be removed as soon as a staff person is no longer employed by the WDFHT/WDFHO.

Principle 8 – Openness about Privacy Policy

The WDFHT and WDFHO will make available to its patients and clients, information regarding the policies and practices relating to the management of personal information in a format that is generally understandable. The Privacy Policy is summarized in the Statement of Information Practices in the clinic waiting room and on the WDFHT website.

Principle 9 – Individual Access
Upon request, an individual will be informed of the existence, use and disclosure of personal information and will be granted access to that information, unless the Executive Director deems that access to that information could be harmful to the patient or a third party.

Principle 10 – Challenging Compliance with the Privacy Policy
The Executive Director will investigate all complaints. If a complaint is found to be justified, appropriate measures will be taken, including amending its policies and practices if necessary.

DEFINITIONS:

Personal Health Information is "identifying" information about an individual's health or health care history. It includes:

- The individual's physical or mental health, including family history
- The provision of health care to the individual
- Long-term care services
- The individual's health care number
- Blood or body part donations
- Payment of eligibility for health care
- The identity of a health care provider or a substitute decision maker for the individual.

A health information custodian (HIC) is an individual or organization that, as a result of their power or duties, has custody or control of personal health information.

Examples of health information custodians include

- Health care practitioners (family physicians, nurses, social workers, dietitians, etc)
- Hospitals, including psychiatric facilities
- Pharmacies
- Laboratories
- Nursing homes, retirement homes and long term care facilities
- Community Care Access Centres
- Ambulance services
- Ministry of Health and Long Term Care

The **Circle of Care** is not a defined term under PHIPA. It is a term of reference used to describe health information custodians and their authorized agents who are permitted to rely on an individual's implied consent when collecting, using, disclosing or handling personal health information for the purpose of providing direct health care.

In a Family Health Team, the circle of care can include:

- Physicians
- Nurses
- Specialist or other health care providers
- Health care professionals selected by the patient (eg pharmacist)

Consent

Express consent may be given verbally, in writing or by electronic means.
Implied consent permits a health care custodian to infer from the surrounding circumstances that an individual would reasonably agree to the collection, use of disclosure of his/her personal health information.

Express consent is always required in certain circumstances.

- E.g., for disclosure of personal health information to an individual or organization that is not a health information custodian and is outside the circle of care (eg. insurance company)
- When information is disclosed by one custodian to another for a purpose other than providing or assisting in providing health care
- When a health information custodian provides information other than name and address for marketing, fund raising, or research purposes.

RELEVANT FORM(S):

Personal Health Information Protection Act 2004
Quality of Care Information Protection Act 2004